

IN THE CLAIMS:

Please amend the claims as indicated in the complete listing of pending claims listed below.

1. (currently amended) A cryptographic method, including:  
receiving at a first entity a second public key  $M_A$ ;  
generating ~~at least one of~~ a first session key  $K_B$  ~~and a first secret  $S_B$~~  based on the second public key  $M_A$ ;  
generating a first random nonce  $N_B$ ;  
encrypting the first random nonce  $N_B$  ~~with at least one of the first session key  $K_B$  and using at least a first password  $P_B$  and a first public key  $M_B$  the first secret  $S_B$~~  to obtain an encrypted random nonce;  
transmitting the encrypted random nonce from the first entity;  
~~receiving a response to transmitting the encrypted random nonce; and authenticating through determining, receiving at the first entity a data signal whether the response includes containing a correct modification of the first random nonce  $N_B+1$ ; and~~  
~~if the received modification of the first random nonce  $N_B+1$  was correctly performed then performing at least one of~~  
~~(i) opening a communication link at the first computer, and~~  
~~(ii) generating a first initialization vector  $I_B$ .~~
2. (currently amended) The method of claim 1 which includes determining whether the ~~received modification was correctly performed wherein said encrypting the first random nonce  $N_B$  includes~~:

generating a first secrete  $S_B$  from at least the first password  $P_B$  and the first public key

$M_B$ ; and

encrypting the first random nonce  $N_B$  using at least the first secrete  $S_B$ .

3. (currently amended) The method of claim 2 wherein ~~determining whether the received modification was correctly performed includes~~said authenticating includes: checking whether ~~the a~~ received modification of the first random nonce  $N_B+1$  equals a modification of the first random nonce  $N_B+1$  as applied to the first random nonce  $N_B+1$  by the first entity.
4. (currently amended) The method of claim 2 wherein ~~determining whether the received modification was correctly performed includes~~said authenticating includes: checking whether ~~the a~~ received modification of the first random nonce  $N_B+1$  less a modification thereof as applied thereto by the first entity equals the first random nonce  $N_B+1$ .
5. (currently amended) The method of ~~claim 1~~claim 2 wherein generating the first session key  $K_B$  ~~includes~~includes:  
~~presenting a numeric parameter  $\beta_B$ ,~~  
generating a first random number  $R_B$ , and  
~~setting computing the first session key  $K_B$  equal to from~~ the second public key  $M_A$  raised to the exponential power of the first random number  $R_B$ , modulo a parameter  $\beta_B$ .

6. (currently amended) The method of claim 1 claim 2 wherein generating the first secret  $S_B$  ~~is generated includes employing using~~ a combining function, function  $f_B$  on at least the first password  $P_B$  and the first public key  $M_B$ .
7. (currently amended) The method of claim 6 wherein ~~employing the combining function,  $f_B$ , includes the first secret  $S_B$  is generated generating a first public key  $M_B$ , using the combining function  $f_B$  function,  $f_B$ , then being employed on a on the first password  $P_B$  and on at least one of the second public key  $M_A$  and the first public key  $M_B$~~ .
8. (currently amended) The method of claim 7 claim 2 wherein ~~employing the combining function,  $f_B$ , on a first password  $P_B$  and on at least one of the second public key  $M_A$  and the first public key  $M_B$  includes said generating the first secrete  $S_B$  includes:~~

combining the second public key  $M_A$  and the first public key  $M_B$  with the first password  $P_B$  to produce a first result, and  
hashing the first result with a secure hash.
9. (original) The method of claim 8 wherein the secure hash is a one-way hash function.
10. (original) The method of claim 9 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvenny Standard.

11. (currently amended) The method of ~~claim 6~~ claim 2 wherein ~~said generating the first secrete S<sub>B</sub> includes: employing the combining function, f<sub>B</sub>, includes employing a plurality of combining functions to produce the first secret S<sub>B</sub>, wherein each of the plurality of combining function produces a prior result, wherein employing a first combining function includes~~  
~~generating a first public key M<sub>B</sub>, and~~  
~~employing the first combining function on a~~ the first password P<sub>B</sub> and ~~on~~ at least one of the second public key M<sub>A</sub> and the first public key M<sub>B</sub> to generate a first combined result, and  
~~employing each subsequent combining functions includes~~  
~~employing a combining function on a prior~~ the first combined result and ~~on~~ at least one of the second public key M<sub>A</sub>, the first password P<sub>B</sub>, and the first public key M<sub>B</sub> to generate a second combined result, wherein the prior result produced by the last combining function is the first secrete S<sub>B</sub>.
12. (currently amended) The method of ~~claim 6~~ claim 2 wherein ~~encrypting the first random nonce N<sub>B</sub> includes employing~~ is encrypted using a symmetrical encryption algorithm.
13. (original) The method of claim 12, wherein the symmetrical encryption algorithm is one of the Data Encryption Standard and the block cipher CAST.
14. (currently amended) The method of claim 2 ~~claim 6~~ wherein encrypting the first random nonce N<sub>B</sub> includes superencrypting the first random nonce N<sub>B</sub>.

15. (currently amended) The method of claim 14, wherein superencrypting the first random nonce  $N_B$  ~~includes~~includes:  
~~superencrypting encrypting~~ the first random nonce  $N_B$  with ~~the first session key  $K_B$~~   
and at least one of the second public key  $M_A$ , a parameter  $\alpha_B$ , a parameter  $\beta_B$ ,  
~~a first public key  $M_B$ , the first session key  $K_B$ , a first password  $P_B$ , and the~~  
first secret  $S_B$  to produce the first encrypted result; and  
encrypting the first encrypted result using the first session key  $K_B$ .
16. (currently amended) The method of ~~claim 1~~claim 2 wherein said transmitting the encrypted random nonce from the first entity ~~includes~~includes:  
transmitting to a second entity ~~a first~~the first public key  $M_B$  to establish the session  
key at the second entity; and  
wherein said authenticating includes:  
decrypting the response using the first session key  $K_B$  ~~the received signal is~~  
~~encrypted based on at least one of a second session key  $K_B$  and a~~  
~~second secret  $S_B$ , and wherein the second session key  $K_B$  and the~~  
~~second secret  $S_B$  are based on the first public key  $M_B$  to generate a first~~  
decrypted result; and  
decrypting the first decrypted result using the first secret  $S_B$ .
17. (currently amended) The method of ~~claim 1~~claim 2, wherein the response includes  
~~signal further includes~~ a combination of a second random nonce  $N_A$  and a  
modification of the first random nonce; and wherein, ~~subsequent to generating the~~  
~~first initialization vector  $I_B$~~ , the method further including includes:  
extracting the second random nonce  $N_A$  from the response;

modifying the second random nonce  $N_A$  to obtain a modified second random nonce  $N_{A_B} + 1$ ;  
encrypting the modified second random nonce  $N_{A_B} + 1$  with at least one of using the first session key  $K_B$  and the first secret  $S_B$  to obtain an encrypted package; and transmitting the encrypted package from the first computer; entity.  
~~in response to transmitting the encrypted random nonce, receiving at the first computer a request to open a communication channel; and opening the communication channel.~~

18. (currently amended) The method of claim 17 wherein said encrypting the modified second random nonce  $N_{A_B} + 1$  ~~includes~~ includes:  
generating a string of random bits  $I_B$ ;  
encrypting it with the first initialization vector  $I_B$ , a combination of the string of random bits  $I_B$  and the modified second random nonce using the first secret  $S_B$  to generate a first result; and  
encrypting the first result using the first session key  $K_B$ .
19. (currently amended) The method of claim 17 wherein the encrypted package is transmitted for authentication of the first entity in opening communication channel is a two-way communication channel.
20. (currently amended) A computer readable storage medium containing executable computer program instructions which, when executed, cause a first computer system to perform a cryptographic method including:  
receiving at the first computer system a second public key  $M_A$ ;

generating ~~at least one of~~ a first session key  $K_B$  ~~and a first secret  $S_B$~~  based on the second public key  $M_A$ ;

generating a first random nonce  $N_B$ ;

encrypting the first random nonce  $N_B$  ~~with at least one of the first session key  $K_B$  and using at least a first password  $P_B$  and a first public key  $M_B$  the first secret  $S_B$~~  to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first computer system;

authenticating through determining whether a in-response to transmitting the encrypted random nonce, receiving at the first computer system a data signal includes containing a correct modification of the first random nonce  $N_B+1$ ; and

~~if the received modification of the first random nonce  $N_B+1$  was correctly performed than performing at least one of~~

(i) ~~opening a communication link at the first computer system and~~

(ii) ~~generating a first initialization vector  $I_B$ .~~

21. (currently amended) A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a computer cryptographic method through a network, the method comprising:

receiving ~~at a~~ ~~at the~~ first computer system a second public key  $M_A$ ;

generating ~~at the first computer system~~ ~~at least one of~~ a first session key  $K_B$  ~~and a first secret  $S_B$~~  based on the second public key  $M_A$ ;

generating ~~at the first computer system~~ a first random nonce  $N_B$ ;

encrypting at the first computer system the first random nonce  $N_B$  with at least one of the first session key  $K_B$  and using at least a first password  $P_B$  and a first public key  $M_B$  the first secret  $S_B$  to obtain an encrypted random nonce; transmitting the encrypted random nonce and the first public key  $M_B$  from the first computer system to the second computer system to establish the session key at the second computer system; receiving at the first computer system from the second computer system a response to transmitting the encrypted random nonce; and authenticating the second computer system at the first computer system through determining, receiving at the first computer system a data signal whether the response includes containing a correct modification of the first random nonce  $N_B+1$ ; and if the received modification of the first random nonce  $N_B+1$  was correctly performed then performing at least one of (i) opening a communication link between the first computer system and the second computer system, and (ii) generating a first initialization vector  $I_B$ .

22. (currently amended) A computer system for performing a cryptographic method through a network, the computer system comprising:  
a processor;  
a network interface coupled to the network and coupled to the processor, the network interface receiving a page to receive a request including information on at least one of a user identification and a user password; and

a file storage device coupled to the processor, the file storage device to store storing  
copies of at least one of a user identification and a user password  
corresponding to the user identification under control of a file management  
system, and wherein the processor is to perform performs a method, including  
including:

receiving ~~at the processor~~ a second public key  $M_A$  through the network  
interface;

generating ~~at least one of~~ a first session key  $K_B$  and ~~a first secret~~  $S_B$ -based on  
the second public key  $M_A$ ;

generating a first random nonce  $N_B$ ;

encrypting the first random nonce  $N_B$  ~~with at least one of the first session key~~  
 ~~$K_B$  and using at least the user password and a first public key~~  $M_B$ , ~~the~~  
~~first secret~~  $S_B$ -to obtain an encrypted random nonce;

transmitting the encrypted random nonce ~~from the processor and the first~~  
public key  $M_B$  through the network interface;

authenticating through determining whether a in response to transmitting the  
encrypted random nonce, ~~receiving at the processor a data signal~~  
~~containing includes a correct~~ modification of the first random nonce  
 $N_B+1$ ; and

~~if the received modification of the first random nonce  $N_B+1$  was correctly~~  
~~performed then performing at least one of~~

(i) ~~opening a communication link at the processor and~~

(ii) ~~generating a first initialization vector  $I_B$ .~~

23. (currently amended) The computer system of claim 22 wherein the network ~~may be is~~

a network operating according to a hypertext transfer protocol; and the first public key  $M_B$  is transmitted with the encrypted random nonce for session key exchange.

24. (currently amended) A cryptographic method, comprising:
    - receiving at a first entity a second public key  $M_A$  and a second random number  $N_A$  encrypted with a second password  $P_A$ ;
    - generating at least one of a first session key  $K_B$  and a first secret  $S_B$  based on the second public key  $M_A$ ;
    - decrypting, employing using at least a first password  $P_B$  and the second public key  $M_A$ , to retrieve the a second random number  $N_A$  from the encrypted second random number  $N_A$  encrypted with the second password  $P_A$ ;
    - modifying the second random number  $N_A$  to obtain a modified second random number  $N_{A+1}$ ;
    - encrypting the modified second random number  $N_{A+1}$  with using at least one of the first password  $P_B$  and a first public key  $M_B$ , first session key  $K_B$  and the first secret  $S_B$  to obtain an encrypted random package; and
    - transmitting the encrypted random package from the first entity; and
    - in response to transmitting the encrypted random package, at least one of
      - (i) receiving at the first entity a request to open a communication link, and
      - (ii) receiving at the first entity an encrypted data package.
25. (currently amended) The method of claim 24, wherein said decrypting includes:  
decrypting receiving the encrypted second random number  $N_A$  using the first session key  $K_B$  to generate a first decrypted result; and  
decrypting the first decrypted result using at least the first password  $P_B$  and the

~~second public key  $M_A$  encrypted with the second password  $P_A$  includes receiving the second random number  $N_A$  superencrypted with the second password  $P_A$  and at least one of the second password  $P_A$ , the second public key  $M_A$ , a parameter  $\alpha_A$ , and a parameter  $\beta_B$ .~~

26. (currently amended) The method of claim 24 wherein said generating the first session key  $K_B$  ~~includes~~ includes:  
~~presenting a numeric parameter  $\beta_B$ ;~~  
generating a first random number  $R_B$ , and  
~~computing setting~~ the first session key  $K_B$  ~~equal to from the first~~ second public key  $M_A$  raised to the exponential power of the first random number  $R_B$ , modulo a parameter  $\beta_B$ .
27. (currently amended) The method of claim 24 wherein said decrypting includes:  
generating ~~the~~ a first secret  $S_B$  ~~includes employing~~ using a combining function ~~function,  $f_B$  on at least~~ the first password  $P_B$  and the second public key  $M_A$ .
28. (currently amended) The method of claim 27 wherein the first secret  $S_B$  is generated employing the combining function  ~~$f_B$ , includes~~  
generating a first public key  $M_B$ , and  
~~employing~~ using the combining  ~~$f_B$  function,  $f_B$ , on a~~ the first password  $P_B$  and on at least one of the second public key  $M_A$  and the first public key  $M_B$ .

29. (currently amended) The method of claim 28 wherein said generating the first secret S<sub>B</sub> employing the combining function, f<sub>B</sub>, on a first password P<sub>B</sub> and on at least one of the second public key M<sub>A</sub> and the first public key M<sub>B</sub> includes includes: combining the second public key M<sub>A</sub> and the first public key M<sub>B</sub> with the first password P<sub>B</sub> to produce a first result, and hashing the first result with a secure hash.
30. (original) The method of claim 29 wherein the secure hash is a one-way hash function.
31. (original) The method of claim 30 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvenny Standard.
32. (currently amended) The method of claim 27 wherein employing the combining function, f<sub>B</sub>, includes employing a plurality of combining functions to produce said generating the first secret S<sub>B</sub>, wherein each of the plurality of combining function produces a prior result, wherein employing a first combining function includes includes: generating a first public key M<sub>B</sub>, and employing the first combining function on a the first password P<sub>B</sub> and on at least one of the second public key M<sub>A</sub> and the first public key M<sub>B</sub> to generate a first combined result, and employing each subsequent combining functions includes

~~employing a combining function on a prior result and on at least one of the second public key  $M_A$ , the first password  $P_B$ , and the first public key  $M_B$  to generate a second combined result, wherein the prior result produced by the last combining function is the first secret  $S_B$ .~~

33. (currently amended) The method of claim 24, wherein said encrypting the modified second random number  $N_{A_B} + 1$  includes superencrypting the modified second random number  $N_{A_B} + 1$ .
34. (currently amended) The method of claim 24, further including:  
generating a first random number  $N_B$  ~~wherein; and~~  
~~wherein said~~ encrypting the modified second random number  $N_{A_B} + 1$  ~~includes~~  
includes:  
encrypting ~~as a first data signal~~ a combination of the first random number  $N_B$  and the modified second random number  $N_{A_B} + 1$ , and ~~wherein~~  
~~receiving at the first computer an encrypted data package includes receiving a second data signal encrypted to at least one of a second session key  $K_A$  and a second secret  $S_A$ , the second data signal including a second initialization vector  $I_A$  and a modified first random nonce  $N_B + 1$ ;~~  
~~retrieving the modified first random nonce  $N_B + 1$  from the encrypted data package;~~  
~~and~~  
~~if the retrieved modification of the first random nonce  $N_B + 1$  less was correctly performed then~~  
~~sending from the first entity a request to open a two way communication channel.~~

35. (currently amended) The method of claim 34 which ~~includes~~ further includes:  
~~receiving at the first entity a response to the encrypted random package;~~  
~~decrypting the response to obtain a combination of a string of random bits and a~~  
~~modified first random nonce; and~~  
~~retrieving the modified first random nonce from the combination of the string of~~  
~~random bits and the modified first random nonce;~~  
determining whether the ~~retrieved modified first random nonce modification~~ was  
correctly ~~performed modified from the first random number N<sub>B</sub>~~.
36. (currently amended) The method of claim 35 wherein said determining whether the  
~~retrieved modification modified first random nonce~~ was correctly modified performed  
~~includes~~ includes:  
checking whether the ~~retrieved modification of the modified~~ first random nonce  $N_B+1$   
equals a modification of the first random nonce as applied to the first random  
nonce  $N_B+1$  by the first entity.
37. (currently amended) The method of claim 35 wherein said determining whether the  
~~received modification modified first random nonce~~ was correctly modified performed  
~~includes~~ includes:  
checking whether the ~~received modification of the modified~~ first random nonce  $N_B+1$   
less a modification thereof as applied thereto by the first entity equals the first  
random nonce  $N_B+1$ .
38. (currently amended) A computer readable storage medium containing executable  
computer program instructions which, when executed, cause a first computer system

to perform a cryptographic method including:

receiving at the first computer system a second public key  $M_A$  and a ~~and an encrypted~~ second random number  $N_A$  ~~encrypted with a second password  $P_A$~~ ;

generating ~~at least one of~~ a first session key  $K_B$  and a first secret  $S_B$  based on the second public key  $M_A$ ;

decypting, using at least employing a first password  $P_B$  and the second public key  $M_A$ , to retrieve the second random number  $N_A$  from the encrypted second random number  $N_A$  ~~encrypted with the second password  $P_A$~~ ;

modifying the second random number  $N_A$  to obtain a modified second random number  $N_A+1$ ;

encrypting the modified second random number  $N_A+1$  ~~with using~~ at least one of the ~~first session key  $K_B$  and the first secret  $S_B$  the first password  $P_B$  and a first~~ public key  $M_B$  to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system for authentication; and

~~in response to transmitting the encrypted random package, at least one of~~

(i) ~~receiving at the first computer system a request to open a communication link, and~~

(ii) ~~receiving at the first computer system an encrypted data package.~~

39. (currently amended) A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a cryptographic method through a network, the method including:

receiving, from the second computer system and at the first computer system, a second public key  $M_A$  and a ~~and an encrypted~~ second random number  $N_A$  ~~encrypted with a second password  $P_A$~~ ;

generating at least one of a first session key  $K_B$  and a first secret  $S_B$  based on the second public key  $M_A$ ;

~~decrypting, using at least employing~~ a first password  $P_B$  and the second public key  $M_A$ , to retrieve ~~the a~~ second random number  $N_A$  from the ~~encrypted~~ second random number  $N_A$  ~~encrypted with the second password  $P_A$~~ ;

modifying the second random number  $N_A$  to obtain a modified second random number  $N_A+1$ ;

encrypting the modified second random number  $N_A+1$  ~~with using~~ at least one of the first session key  $K_B$  and the first secret  $S_B$  the first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system ~~to the second computer system; and~~

~~in response to transmitting the encrypted random package, at least one of~~

(i) ~~receiving at the first computer system a request to open a communication link, and~~

(ii) ~~receiving at the first computer system an encrypted data package.~~

40. (currently amended) A computer system for performing a cryptographic method through a network, the computer system comprising:
  - a processor;
  - a network interface coupled to the network and coupled to the processor, the network interface ~~receiving a page to receive a request including information on at~~

~~least one of~~ a user identification ~~and a user password~~; and

a file storage device coupled to the processor, the file storage device to store ~~storing~~ copies of ~~at least one of~~ a user identification ~~and a user password~~ associated with the user identification ~~under control of a file management system~~, and wherein the processor performs ~~is to perform~~ a method, including receiving at the processor a second public key  $M_A$  ~~and a~~ ~~and an encrypted~~ second random number  $N_A$  ~~encrypted with a second password  $P_A$~~  through the network interface;

generating ~~at least one of~~ a first session key  $K_B$  ~~and a first secret  $S_B$~~  based on the second public key  $M_A$ ;

decrypting, ~~using at least employing~~ a first password  $P_B$  ~~and the second public key  $M_A$~~  to retrieve the second random number  $N_A$  from the encrypted second random number  $N_A$  ~~encrypted with the second password  $P_A$~~ ;

modifying the second random number  $N_A$  to obtain a modified second random number  $N_A+1$ ;

encrypting the modified second random number  $N_A+1$  ~~with using~~ at least one of the first session key  $K_B$  ~~and the first secret  $S_B$~~  the first password  $P_B$  and a first public key  $M_B$ , to obtain an encrypted random package;

transmitting the encrypted random package ~~from the processor~~ through the network interface; and

in response to transmitting the encrypted random package, at least one of

(i) ~~receiving at the processor a request to open a communication link,~~

and

(ii) ~~receiving at the processor an encrypted data package.~~

41. (currently amended) The computer system of claim 40 wherein the network ~~may be~~ is a network operating according to a hypertext transfer protocol; and the first public key  $M_B$  is transmitted for session key exchange before the encrypted second random number is received.